(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－70576

(43)公開日　平成10年(1998)３月10日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	12/66		9744－5K	Ｈ０４Ｌ	11/20	Ｂ
Ｇ０６Ｆ	13/00	３５３		Ｇ０６Ｆ	13/00	３５３Ｔ
		３５７				３５７Ｚ
Ｈ０４Ｌ	12/24		9744－5K	Ｈ０４Ｌ	11/08	
	12/26					

審査請求　未請求　請求項の数３　ＯＬ　（全７頁）

(21)出願番号　特願平8－227969

(22)出願日　平成８年(1996)８月29日

(71)出願人　000001214
国際電信電話株式会社
東京都新宿区西新宿２丁目３番２号

(72)発明者　塩田　歩
東京都新宿区西新宿二丁目３番２号　国際電信電話株式会社内

(72)発明者　片岸　一起
東京都新宿区西新宿二丁目３番２号　国際電信電話株式会社内

(72)発明者　浅見　徹
東京都新宿区西新宿二丁目３番２号　国際電信電話株式会社内

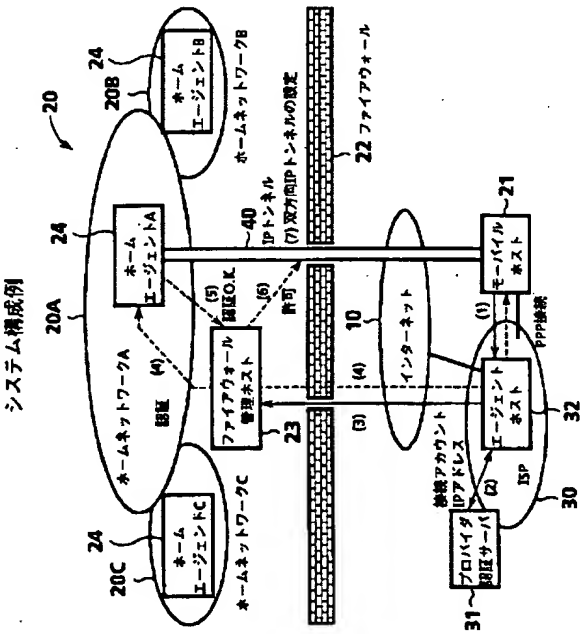
(74)代理人　弁理士　光石　俊郎　（外２名）

(54)【発明の名称】　ファイアウォール動的制御方法

(57)【要約】

【課題】　インターネットサービスプロバイダ（ＩＳＰ）にダイヤルアップ接続中の移動端末及びそのユーザに対してファイアウォールのフィルタ設定を適切に行い、更に、ホームネットワーク資源へのアクセスを適切に許可できること。

【解決手段】　ＩＳＰ３０にダイアルアップにより接続中の端末２１がインターネット１０を経由してファイアウォール２２内の内部ネットワーク２０にアクセスする際に、ＩＳＰ３０から端末２１のユーザ情報を送り、このユーザ情報を基に端末２１が内部ネットワーク２０から移動した移動端末であるか否かを判断し、移動端末である場合に、同端末２１と内部ネットワーク２０との通信を許可するようにファイアウォール２２のフィルタを設定し、更に、同端末２１と内部ネットワーク２０との通信をＩＰトンネル４０により行う。



1

【特許請求の範囲】
【請求項１】　インターネットサービスプロバイダにダイアルアップにより接続中の端末がインターネットを経由してファイアウォール内の内部ネットワークにアクセスする際に、前記インターネットサービスプロバイダから前記内部ネットワークに前記端末のユーザ情報を送ること、前記内部ネットワークはこのユーザ情報を基に前記端末が同内部ネットワークから移動した移動端末か否かを判断すること、前記端末が移動端末である場合に同端末と内部ネットワークとの通信を許可するようにファイアウォールのフィルタを設定することを特徴とするファイアウォール動的制御方法。
【請求項２】　前記フィルタの設定後、前記端末と内部ネットワークとの通信をＩＰトンネルにより行うことを特徴とする請求項１に記載のファイアウォール動的制御方法。
【請求項３】　前記端末のユーザ情報の送信をインターネットサービスプロバイダに設けたエージェントホストと内部ネットワークに設けたファイアウォールのフィルタの設定を行うファイアウォール管理用ホストとの間で行うこと、前記ＩＰトンネルによる通信を前記端末と内部ネットワークに設けたホームエージェントとの間で行うことを特徴とする請求項２に記載のファイアウォール動的制御方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明はファイウォールを動的に制御する方法に関する。
【０００２】
【従来の技術】社内ネットワークをインターネットに接続している場合、インターネットからの不正アクセスを防ぐ必要がある。但し、外部ネットワークと内部ネットワーク間の通信を完全に遮断すると、ユーザが外出先からインターネット経由でホームネットワークにアクセスしようとしても、これが不可能になる。
【０００３】（ファイアウォールとフィルタ処理）そのため、インターネットを経由した外部からの通信を選択的に通過させるファイアウォール（防火壁）の構築が必須となっている。
【０００４】従来、ファイアウォールでは、内部ネットワークと外部ネットワークの間で通信されるデータパケットの内、予め許可されているパケットのみを通し、それ以外のパケットを遮断するというフィルタ処理が行われている。
【０００５】フィルタの設定は、通常、送信元端末のＩＰ（Internet Protocol:インターネット通信規約）アドレス、送信先端末のＩＰアドレス、使用プロトコルの種類、及び、ポート番号等を指定することにより行われる。例えば、外部の特定ＩＰアドレスから内部の任意ホスト（端末）へのＴＣＰ（Transmission Control Protocol:伝送制御通信規約）プロトコルによる通信を行う場合、或るポート番号（例えば１１０）を使用しているものに限って許可するといった設定がなされる。

2

【０００６】なお、ポート番号とは、ＴＣＰ、ＵＤＰ（User Datagram Protocol）において上位層のプロセスを特定するために使用する識別子である。
【０００７】しかし、ノート型パソコン等の携帯型コンピュータをユーザが持ち歩き、移動先でインターネットサービスプロバイダ（ＩＳＰ（Internet Service Provider)と略記する）経由のダイヤルアップ接続（ＰＰＰ接続とも称される）によりインターネットに接続して、ホームネットワークへのアクセスを行う場合は、適切なフィルタ処理を行うことが難しい。
【０００８】これは、インターネットの通信に用いられるＩＰアドレスは４バイトの数値で表されるが、その上位桁部分は端末が接続されているネットワークを表し、下位部分がそのネットワーク内での当該端末の識別番号になっているためである。つまり、ホームネットワークから移動した端末（モーバイルホスト：ＭＨ（MobileHost)と略記する）でダイヤルアップ接続を行う場合は、その移動端末に割り当てられるＩＰアドレスが接続の度に変わり、ホームネットワークでのＩＰアドレスをそのまま使用して通信を行うことができない。このようにダイヤルアップ接続の場合は移動端末のＩＰアドレスが一定しないことから、、ファイアウォールにおいてデータパケットの送信元端末のＩＰアドレス及び送信先端末のＩＰアドレスを特定してフィルタを設定することが不可能になる。
【０００９】しかも、仮にファイアウォールのフィルタ設定を適切に行い、権限を持つ移動端末及びそのユーザによる外部から内部へのアクセスのみを許可することが可能になったとしても、同ユーザが普段ホームネットワークでアクセスしている共有ディスク、社内データベース、及び、ＷＷＷ（World Wide Webの略)の社内向けページといった各種内部ネットワーク資源の利用が可能になるとは限らない。
【００１０】何故ならば、これら内部ネットワーク資源には個別にアクセス制限が行われている場合があり、その際、クライアント端末のＩＰアドレスに基づいてアクセスの許可及び不許可を決める場合が多いからである。
【００１１】（モーバイルＩＰ）次に、現在標準化が進められているモーバイルＩＰ（Mobile-IP)を、図３を参照して説明する。モーバイルＩＰとは、端末が何処に移動してインターネットに接続しても、他の端末が当該移動端末に対して、常に同じＩＰアドレスを用いて通信を行うことを可能にする技術である。但し、現状のモーバイルＩＰは仕様上、ファイアウォールを持つネットワークには未対応である。
【００１２】図３において、１００はインターネット、２００は移動端末２０１のホームネットワーク、２０２

はホームネットワーク２００上のホームエージェント（ＨＡ（Home Agent）と略記する）、２０３はルータ、３００はＩＳＰ、４００は他のネットワーク、４０１は他のネットワーク４００上の端末をそれぞれ示す。

【００１３】ここでは、移動端末２０１が通常接続されているホームネットワーク２００のＩＰアドレスを［133.128.8.0]とし、同ホームネットワーク２００における移動端末２０１のＩＰアドレスを［133.128.8.81］とし、ホームエージェント２０２のＩＰアドレスを［133.128.8.100]とし、移動端末２０１がＩＳＰ３００にダイアルアップ接続した時に割り当てられるＩＰアドレスを［130.54.20.199]としている。

【００１４】一般に、或るネットワーク４００の端末４０１から端末２０１宛にパケットが送出されると、図３中に符号５０１で示す経路のように、端末２０１が通常接続されているホームネットワーク２００に配送される。そのため、端末２０１が別のネットワーク例えばＩＳＰ３００に移動している場合には、パケットを移動先のネットワーク３００に転送する必要がある。

【００１５】この転送を行うため、モーバイルＩＰでは、移動元のネットワークと移動先のネットワークにそれぞれエージェントホストが設置される。移動元ネットワークに設置されるエージェントホストはホームエージェントと呼ばれる。移動先のネットワークに設置されるエージェントホストはフォーリンエージェント（ＦＡ（Foregin Agent)と略記する）と呼ばれる。移動端末自身がフォーリンエージェントの役割を果たすことも可能である。図３では、移動端末２０１がフォーリンエージェントの機能を有するものとしている。

【００１６】端末２０１がホームネットワーク２００から移動してＩＳＰ３００にダイアルアップ接続３０１を行うと、ＩＳＰ３００から一時的なＩＰアドレス［130.54.20.199]が割り当てられる。

【００１７】そこで、移動端末２０１はこのＩＰアドレスと、通常接続しているホームネットワーク２００におけるＩＰアドレス［133.128.8.81］とをＩＳＰ３００及びインターネット１００を経由してホームネットワーク２００のホームエージェント２０２に通知しておく。これにより、ホームエージェント２０２はＩＰアドレス［133.128.8.81］を持つ端末２０１が移動中であり、それが一時的に取得したＩＰアドレスが［130.54.20.199]であることを知るので、データベースに記録しておく。

【００１８】そして、或るネットワーク４００内の端末４０１から通常のＩＰアドレス［133.128.8.81］を用いて端末２０１宛のパケットが届くと、端末２０１の代わりにホームエージェント２０２が受け取る（経路５０２参照）。ホームエージェント２０２は、端末４０１から移動端末２０１宛の前記パケットを、一時的に取得したＩＰアドレス［130.54.20.199]向けのパケットに埋め込み、インターネット１００及びＩＳＰ３００を経由して

移動端末２０１に転送する（経路５０３参照）。移動端末２０１は受け取ったパケットから元のパケットを取り出し、必要に応じて送信元の端末４０１宛にＩＳＰ３００及びインターネット１００を経由してパケットを送る（経路５０４参照）。

【００１９】上述の如く、モーバイルＩＰによれば、端末４０１からは移動中の端末２０１に、それの通常のＩＰアドレス［133.128.8.81］を用いてパケットを送ることができる。

【００２０】しかし、移動端末２０１とホームエージェント２０２との間では、一時的に取得したＩＰアドレス［130.54.20.199]を用いて通信が行われる。

【００２１】つまり、現状のモーバイルＩＰでは、移動端末２０１が送出するパケットには一時的に取得したＩＰアドレスを用いて何らの処理も加えないため、通常通りルーティングされる。従って、前述したフィルタ処理によるファイアウォールの設定では、移動端末２０１とホームエージェント２０２間の通信のみを許可するので、移動端末２０１がホームエージェント２０２以外のホームネットワーク２００内の内部ホスト（端末）と通信を行うことができない。これは、各種内部ネットワーク資源への移動端末２０１のアクセスが制限されることを意味する。

【００２２】

【発明が解決しようとする課題】本発明は上記問題点に鑑み、インターネットサービスプロバイダ（ＩＳＰ）にダイヤルアップ接続中の移動端末及びそのユーザに対して適切なフィルタ設定を行うことができるファイアウォール動的制御方法、並びに、同端末及びユーザが外部からホームネットワーク資源へアクセスすることを適切に許可することができるファイアウォール動的制御方法を提供することを目的とする。

【００２３】

【課題を解決するための手段】まず本発明では、インターネットサービスプロバイダからユーザ情報を得ることにより、このユーザ情報を基にフィルタの設定を適切に行うことを可能にする。また本発明では、このフィルタ設定に、現在標準化が進められているモーバイルＩＰの技術を改良して組み合わせることにより、ホームネットワーク資源へのアクセス制限の問題を解決する。

【００２４】即ち、本発明のファイアウォール動的制御方法は、インターネットサービスプロバイダにダイアルアップにより接続中の端末がインターネットを経由してファイアウォール内の内部ネットワークにアクセスする際に、前記インターネットサービスプロバイダから前記内部ネットワークに前記端末のユーザ情報を送ること、前記内部ネットワークはこのユーザ情報を基に前記端末が同内部ネットワークから移動した移動端末か否かを判断すること、前記端末が移動端末である場合に同端末と内部ネットワークとの通信を許可するようにファイアウ

ォールのフィルタを設定することを特徴とする。

【００２５】また、本発明のファイアウォール動的制御方法は、前記フィルタの設定後、端末と内部ネットワークとの通信をＩＰトンネルにより行うことを特徴とし、或いは、更に前記端末のユーザ情報の送信をインターネットサービスプロバイダに設けたエージェントホストと内部ネットワークに設けたファイアウォールのフィルタの設定を行うファイアウォール管理用ホストとの間で行うこと、前記ＩＰトンネルによる通信を前記端末と内部ネットワークに設けたホームエージェントとの間で行うことを特徴とする。

【００２６】

【発明の実施の形態】以下、図１と図２を参照して本発明の実施の形態を説明する。図１は本発明のファイアウォール動的制御方法を適用したシステム構成例を示す図、図２はファイアウォールに対応したモーバイルＩＰの説明図である。

【００２７】図１において、１０はインターネット、２０は複数のホームネットワーク２０Ａ、２０Ｂ、２０Ｃを有する或る内部ネットワーク、２１は通常内部ネットワーク２０に接続されている移動端末、２２はファイアウォール、２３はファイアウォール管理用ホスト、２４は各ホームネットワーク２０Ａ、２０Ｂ、２０Ｃに設けたホームエージェント、３０はＩＳＰ（インターネットサービスプロバイダ）、３１はＩＳＰ３０のプロバイダ認証サーバ、３２はＩＳＰ３０のエージェントホストをそれぞれ示す。

【００２８】移動端末２１はモーバイルＩＰ用のフォーリンエージェント機能を有し、移動先でＩＳＰ３０にダイアルアップ接続し、インターネット１０を介して内部ネットワーク２０に接続しようとしているものとする。

【００２９】本実施例では、以下のようにして、ＩＳＰ３０から得るユーザ情報を基にファイアウォールの制御を行う機構と、ファイアウォール２２に対応させたモーバイルＩＰの機構を用意している。

【００３０】（ファイアウォールの動的制御機構）まず、図１を参照して、ＩＳＰ３０から得るユーザ情報を基にファイアウォール２２の制御を行うファイアウォールの動的制御機構の構成を説明する。

【００３１】移動端末２１のユーザがＩＳＰ３０へダイアルアップ接続する際には、ユーザアカウント（ＩＤ）とパスワードを入力する。ＩＳＰ３０では、ユーザの入力データが適正か否かをプロバイダ認証サーバ３１により判定し、適正な場合にのみ、移動端末２１にＩＰアドレスを割り当ててインターネット１００に接続する。そのため、ＩＳＰ３０側では、ユーザアカウントとパスワードを基にどのようなユーザが現在ダイアルアップで接続中であるか、また、その移動端末２１にはどのＩＰアドレスを割り当てたかというユーザ情報を常に把握できてている。

【００３２】そのため、このユーザ情報をＩＳＰ３０側から内部ネットワーク２０が取得して、現在どのユーザがどのＩＰアドレスを使っているかが判れば、前述のフィルタの設定を適切に行うことが可能になる。これにより、内部ネットワーク２０へのアクセスが予め許されたユーザからの通信のみを許可し、内部へのアクセス権限のないユーザからのアクセスを排除することができる。

【００３３】そこで、図１に示すように、ファイアウォール管理用ホスト２３を内部ネットワーク２０に設けることにより、フィルタの追加・削除を行う機構を用意する。また、ＩＳＰ３０側にエージェントホスト３２を設け、このエージェントホスト３２とファイアウォール管理用ホスト２３間の通信のみを許可しておく。この通信には、ファイアウォール管理用ホスト２３もエージェントホスト３２も固定したＩＰアドレスを用いることができるので、ファイアウォール用フィルタ設定に何の障害もない。具体的には、下記（１）～（７）の手順が採られる。なお、下記手順（ｎ）は図１中の同記号（ｎ）に対応している。

【００３４】（１）外部から内部へのアクセスを行う移動端末２１は、ＩＳＰ３０のエージェントホスト３２経由で、内部ネットワーク２０とのコネクション確立要求を行う。

（２）エージェントホスト３２は、移動端末２１のＩＰアドレスとダイアルアップ接続時のアカウントを調べる。

（３）エージェントホスト３２は、移動端末２１がファイアウォール２２内部へのアクセスを許可された特定アカウントで接続されている場合のみ、移動端末２１からのメッセージをファイアウォール管理用ホスト２３に中継する。

（４）モーバイルＩＰでは移動端末とホームエージェントとの間でエンド・ツー・エンドの認証を行うことになっているので、ファイアウォール管理用ホスト２３を通して移動端末２１とホームエージェント２４との間でエンド・ツー・エンドの認証を行う。

（５）この認証が成功すれば、その旨のメッセージをホームエージェント２４がファイアウォール管理用ホスト２３に送る。

（６）この結果、ファイアウォール管理用ホスト２３は移動端末２１とホームエージェント２４間の通信を通過させるように、ファイアウォール２２のフィルタ設定を変更する。

（７）ファイアウォール２２の設定を変更して移動端末２１とホームエージェント２４間の通信を可能にした時点で、ファイアウォール管理用ホスト２３はその旨をホームエージェント２４へ通知するとともに、エージェントホスト３２経由で移動端末２１へも通知する。この通知を受けて、ホームエージェント２４が移動端末２１へのＩＰトンネルを設定し、また、移動端末２１がホーム

エージェント２４へのＩＰトンネルを設定することで、双方向ＩＰトンネル４０が設定される。

【００３５】このＩＰトンネル４０を用いて、移動端末２１が内部ネットワーク２０の各端末との通信を行う。ただし、移動端末２１はコネクションの継続のためのメッセージをファイアウォール管理用ホスト２３へ定期的に送るものとし、継続要求の途絶えたホスト向けのフィルタ設定は、ファイアウォール管理用ホスト２３が自動的に削除するものとしている。

【００３６】以上により、必要な期間のみ、始点と終点が明確に限定された通信のみを許可するファイアウォール２２の設定が可能である。また、双方向ＩＰトンネル４０の設定が可能である。

【００３７】前述の如く、現在標準化が進められているモーバイルＩＰの仕様は、ファイアウォール２２の有るネットワーク２０には対応していない。そのため、モーバイルＩＰをファイアウォール２２に対応するように、下記の如く改良し、前述のフィルタの設定法と組み合わせて用いる。

【００３８】（ファイアウォール対応モーバイルＩＰ）図２を参照して、モーバイルＩＰとファイアウォール動的制御との組み合わせ方について説明する。

【００３９】移動端末２１からファイアウォール２２内部の端末２５へ送信するパケットは、図２中の経路５２のように、ホームエージェント２４宛のパケットに埋め込んで送出す。ホームエージェント２４は、受け取ったパケットから元のパケットを取り出す。そして、ホームエージェント２４は図２中の経路５３のように、元のパケットを再びネットワーク２０に送出することで、本来の宛て先である内部端末２５に配送する。図２中の符号２６はルータを示す。なお、ネットワーク２０内に居る場合には、移動端末２１は経路５１で端末２５と通信する。

【００４０】このように、移動端末２１とホームエージェント２４間で双方向にカプセル化（トンネリング）を行うことにより、ネットワーク２０内で個別にアクセス制限が行われている場合でも、移動端末２１がネットワーク２０に通常接続されている場合のＩＰアドレスに基づいてアクセスを許可できるから、移動端末２１とファイアウォール２２内部の端末２５との通信が可能である。

【００４１】

【発明の効果】本発明によれば、ダイアルアップ接続中の特定ユーザからの通信のみを通過させるようなファイアウォールの設定が、ＩＳＰとの連携により可能である。

【００４２】また、本発明によれば、モーバイルＩＰを改良して組み合わせることにより、外部からでも、内部ネットワークに接続している時と全く同じ権限で、普段利用している内部ネットワーク資源へアクセスすることが可能である。

【図面の簡単な説明】

【図１】本発明のファイアウォール動的制御方法を適用したシステム構成例を示す図。

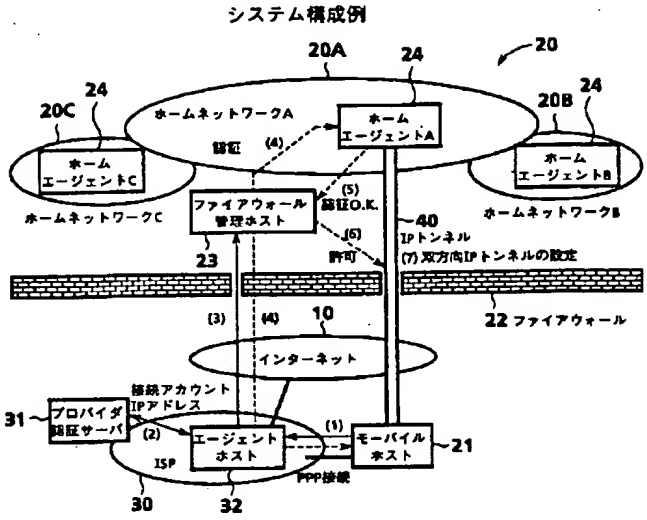
【図２】ファイアウォールに対応したモーバイルＩＰの説明図。

【図３】ファイアウォールに未対応の従来のモーバイルＩＰの説明図。

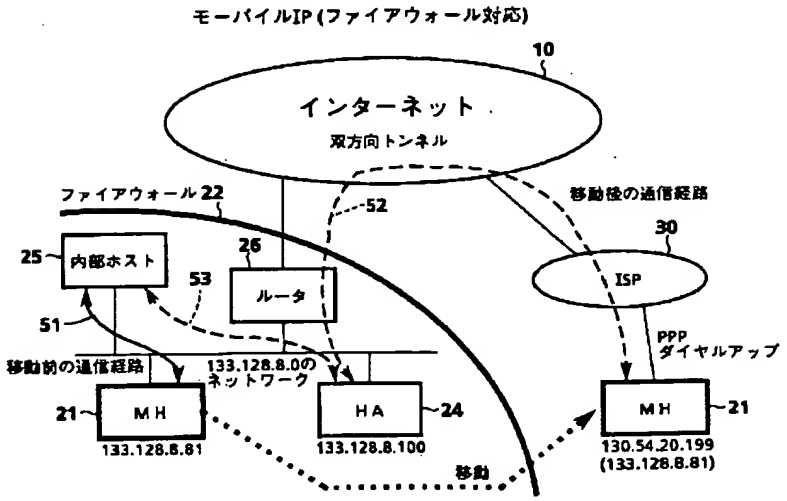
【符号の説明】

１０　インターネット
２０　内部ネットワーク
２０Ａ、２０Ｂ、２０Ｃ　ホームネットワーク
２１　フォーリンエージェント機能を有する移動端末
２２　ファイアウォール
２３　ファイアウォール管理用ホスト
２４　ホームエージェント
２５　内部端末
２６　ルータ
３０　ＩＳＰ（インターネットサービスプロバイダ）
３１　プロバイダ認証サーバ
３２　エージェントホスト
４０　双方向ＩＰトンネル
５１　移動前の通信経路
５２、５３　移動後の通信経路

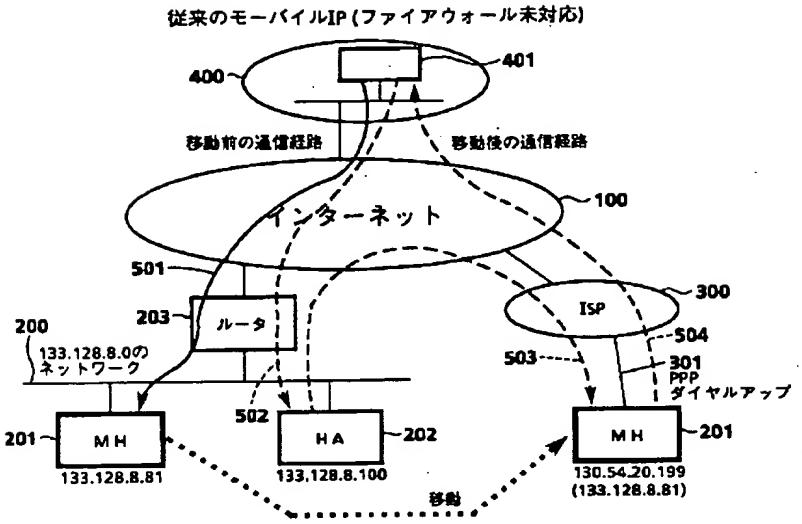
【図１】


システム構成例
20A
24
20
24
20C
ホームネットワークA
ホーム
エージェントA
24
20B
ホーム
エージェントC
(4)
認証
ホーム
エージェントB
(5)
認証O.K.
ファイアウォール
管理ホスト
ホームネットワークC
ホームネットワークB
40
IPトンネル
(6)
許可
(7) 双方向IPトンネルの設定
23
(3)
(4)
10
22 ファイアウォール
インターネット
接続アカウント
IPアドレス
31
プロバイダ
認証サーバ
(2)
(1)
エージェント
ホスト
モーバイル
ホスト
21
ISP
PPP接続
30
32

【図２】


モーバイルIP(ファイアウォール対応)
10
インターネット
双方向トンネル
ファイアウォール 22
52
移動後の通信経路
30
25
内部ホスト
26
ルータ
ISP
53
51
PPP
ダイヤルアップ
移動前の通信経路
133.128.8.0の
ネットワーク
21
MH
HA
24
MH
21
133.128.8.81
133.128.8.100
130.54.20.199
(133.128.8.81)
移動

【図３】


従来のモーバイルIP(ファイアウォール未対応)
400
401
移動前の通信経路
移動後の通信経路
インターネット
100
501
203
ルータ
200
133.128.8.0の
ネットワーク
300
ISP
504
503
301
PPP
ダイヤルアップ
502
201
MH
133.128.8.81
HA
202
133.128.8.100
MH
201
130.54.20.199
(133.128.8.81)
移動